IMT-2000 이동통신시스템에서 망접속보안기능 적용에 따른 무선링크 성능 분석

권 수 근†

요 약

IMT-2000 이동통신시스템에서는 빠른 전송속도의 지원으로 무선인터넷, 전자상거래 등 많은 응용서비스의 제공이 예상된다. 이들 서비스는 인증, 데이터 무결성, 데이터 암호화, 부인방지 등 높은 수준의 보안기능을 요구한다. 본 논문에서는 IMT-2000에서 암호화, 인증 등 망접속 보안기능 제공에 따른 이동국과 기지국간 무선링크의 성능 분석을 수행하였다. 망 접속보안서비스의 지원에 필요한 무선구간의 신호트래픽은 평균메시지의 길이가 256~768bits, 기본서비스 대비 보안서비스 발생율이 0.2~1.0, 기본서비스의 발생율이 0.2~1.0서비스/호 인 조건에서 최소 0.2kbps에서 최대 4.5kbps로 분석되었다.

Performance Analysis of Air Interface for Network Access Security Services in IMT-2000 Mobile Systems

Sookun Kwon†

ABSTRACT

IMT-2000 mobile system will provide many application services such as mobile internet, wireless electronics commerce applications using air interface with high data rate. These applications require high data integrity, data confidentiality, user authentication, user identity confidentiality and non-repudiation. In this study, we analyze air interface performance for network access security services in IMT-2000 mobile systems. Signal traffic for network access security services requires 0.2kbps~4.5kbps with the conditions of 246~768bits/message, 0.2~1.0 basic services/sec and the security services of the rate of 0.2~1.0 times compared with basic services.

1. 서 론

이동통신은 공간의 제약을 받지 않는 서비스의 이점으로 인하여 수요가 폭발적으로 증가하고 있다. 2세대 이동통신시스템인 CDMA방식의 Digital Cellular System(DCS)과 Personal Cellular System(PCS)의 경우 우리나라가 세계최초로 상용화 개발에 성공하였으며, 현재 광범위하게 서비스되고 있다. 2세대 이동통신시스템은 음성서비스는 충분히 제공하고 있으나 점차 수요가 증대되고 있는 영상서비스, 무선인터넷 등 멀티미디어 서비스의 제공에는 한계를 가지고 있다. 이동멀티미디어 서비스를 제공하기 위해 3세대 이동통신시스템인 International Mobile Telecommunications-2000(IMT-2000)이 개발되고 있다. IMT-2000의 무선접속 국제표준으로 광대역 CDMA 방식이 채택되었으며 3GPP, 3GPP2등의 국제표준기구에서 동기 및 비동기방식에 대한 표준화를 진행하고 있으며, 국내에서도 많은 연구가 진행되고 있다[1-4].

보안에 취약한 무선구간을 포함하는 이동통신에서 절대적으로 요구되며, 또한 기존의 음성통신위주에서 무선인터넷서비스, 전자상거래 등의 수요가 음성서비스를 능가하게 될 차세대이동통신의 경우 가

본 연구는 한국과학재단 목적기초연구(2001-1-51200-001-1) 지원으로 수행되었음.
† 정회원, 경주대학교 컴퓨터전자공학부

입자에 대한 인증 및 보안에 대한 연구는 매우 중요한 기술이다[5-8]. 보안을 요구하는 응용서비스를 지원하기 위해 IMT-2000 이동통신시스템에서도 유선에서와 동일한 수준의 사용자 인증, 데이터 무결성 및 기밀성 유지, 부인방지 등의 보안절차가 요구된다. 그러나 IMT-2000과 같은 이동통신시스템에서는 무선링크상의 제한된 대역폭을 고려한 신호메세지 전달의 최소화, 무선자원의 고비용 부담을 고려한 무선대역폭의 효율적인 사용, 이동단말기의 제한된 계산능력 등의 제한요소를 가지며 이에 대한 고려가 필요하다. 지금까지 이동통신을 위한 인증 및 키 설정방식, 암호화, 무결성, 부인방지 등의 서비스시 이동국과 무선링크의 부하를 감소시키기 위한 많은 연구가 진행되고 있다[9-11]. 그러나 셀 설계, 효율적인 무선 프로토콜 설계, 신호채널 설계 등에 필수적으로 요구되는 보안서비스 처리에 따른 무선링크에서의 성능분석에 대한 연구가 미흡하다.

본 논문에서는 IMT-2000에서 요구되는 보안요소의 구조 및 기능을 분석하고, 기본서비스 부하 및 보안기능에 따라 추가적으로 요구되는 무선링크에서의 신호트래픽을 종합적으로 고려한 무선링크의 성능을 분석한다. 본 논문은 다음과 같이 구성된다. II장에서는 IMT-2000의 보안 구조 및 기능을 살펴보고, III장에서는 IMT-2000 무선접속 표준규격을 기반으로 망접속 보안기능의 구성 요소간 기능 할당 모델을 설명한다. IV장에서는 망접속 보안기능 적용에 따른 무선링크 성능을 분석하고 끝으로 V 장에서 결론을 내린다.

2. IMT-2000 보안 구조 및 기능

2.1 IMT-2000 보안 구조

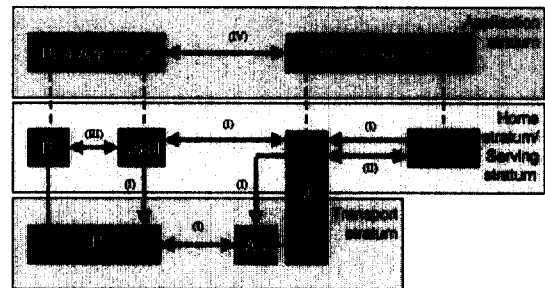
그림 1은 IMT-2000의 보안 구조를 보여준다. IMT-2000 보안서비스 제공을 위해서는 아래의 5개의 기능군으로 정의할 수 있다[1]. 첫째, 망접속 보안(Network access security, I)으로서 IMT-2000 서비스에서 보안 엑세스를 제공하는 기능군으로 특히 무선접속구간에서 침입을 방지한다. 둘째는 망영역 보안(Network domain security, II)으로 서비스 제공자 영역에서 각 노드들간 신호정보들의 안전한 교환을 제공하는 기능군으로 유선망에서의 침입을 방지한다. 셋째, 사용자 영역 보안(User domain security, III)으로 이동국 접속시 보안을 제공하는 기능군이다. 넷째, 응용영역 보안(Application domain security, IV)으로 사용자 및 서비스제공자의 영역에서 응용부의 메시지 교환 보안을 지원하는 기능군이다. 마지막으로 보안기능의 가시성 및 구성능력(Visibility and configurability of security, V)으로 사용자가 보안기능이 수행되고 있는지 여부를 알 수 있는 지와 서비스의 사용 및 제공이 보안기능에 따라 제공되는 기능군이다.

TE : Terminal Equipment
USIM : User Services Interface Module
MT : Mobile Termination
SN : Serving Network
HE : Home Environment

그림 1. IMT-2000 보안 구조

2.2 망접속 보안기능

IMT-2000에서 망접속에 필요한 기능은 사용자 신원의 기밀성, 인증, 데이터 기밀성 및 데이터 무결성 등 크게 네 가지의 보안기능이 요구된다. 사용자 신원의 기밀성은 서비스 대상 사용자의 영구사용자 식별자(IMUI)가 무선링크 상에서 노출되지 않도록 하는 사용자신원 비밀성, 사용자가 어떤 지역에 위치하는지 무선링크 상에서 노출되지 않도록 하는 사용자위치 비밀성, 침입자가 무선 링크를 통해 동일사용자에게 다른 서비스가 전달되는지 추적할 수 없도록 하는 사용자 비추적성(user untraceability)이 요구된다[6]. 위의 목적을 달성하기 위해 사용자는 일반적으로 방문 서비스망에 알려진 임시사용자 식별자에 의하여 확인되거나 암호화된 영구사용자 식별자에 의하여 확인된다. 사용자 신원 노출을 야기하는 사용자의 추적을 피하기 위해 오랜 시간 동안 동일한 임시사용자 식별자나 암호화된 식별자를 사용하지 않아야 한다. 위의 보안기능을 위해 추가적으로 사용

자 신원을 노출시킬 수 있는 신호 및 사용자 정보는 무선 링크 상에서 암호화되어야 한다.

인증과 관련된 요구기능으로 사용자와 서비스 제공망은 안전하게 인증 및 이후에 사용될 키를 협상할 수 있는 인증 메커니즘 등의 절차, 서비스망이 사용자와 협의하여 사용자의 신원을 확인하는 사용자 인증 절차, 사용자가 서비스망이 HE에 의하여 인증된 망인지를 확인하는 망 인증절차 등이 요구된다. IMT-2000에서의 인증은 두 가지의 메커니즘이 제공된다. 하나는 HE에 의하여 서비스망에 전달된 인증벡터를 사용하는 방식이고, 다른 하나는 이전에 수행된 인증 및 키 설정 절차에 따라 사용자와 서비스망간에 설정된 인증키를 사용하여 로컬 인증을 하는 방법이다[6]. 인증 및 키 설정은 로컬인증에 사용되는 유도된 인증키의 최대수가 수행된 경우 서비스망에 첫번째 위치 등록 후, 서비스 요청 후, 위치수정 요청 후, detach request 또는 연결 재설정 요구 후에 서비스망에 의하여 요청된다. 로컬 인증은 사용되는 derived integrity key의 최대수에 도달되지 않은 경우 서비스망에 자체적으로 수행된다.

데이터의 기밀성 유지를 위해 망 엑세스시 이동국과 망이 사용할 암호 알고리즘을 협상할 수 있는 암호 알고리즘 합의 절차, 사용할 암호 키(Ciphering Key)를 협상할 수 있는 암호 키 합의 절차, 사용자 데이터가 무선링크 상에서 노출되지 않도록 하는 사용자 데이터의 기밀성, 신호 데이터가 무선링크 상에서 노출되지 않도록 하는 신호 데이터 기밀성 기능 등이 요구된다. 암호 키 합의는 인증 및 키 합의를 위한 메커니즘의 수행으로 실현되며, 암호 알고리즘의 합의는 사용자와 망간의 보안모드 협상 절차에서 수행된다.

망 엑세스 링크에서 데이터의 무결성 제공을 위해 이동국과 망이 안전하게 무결성 알고리즘을 협의할 수 있는 특성인 무결성 알고리즘 합의 절차, 사용할 무결성 키를 합의하는 무결성 키 합의 절차, 수신엔티티(MS or SN)가 수신한 신호정보가 도중에 허가되지 않은 방법으로 변경되지 않았음을 확인할 수 있는 특성인 데이터 무결성 및 신호데이타의 인증 기능이 요구된다. 무결성 키(Integrity Key) 합의는 인증 및 키 합의를 위한 메커니즘의 수행으로 실현되며, 무결성 알고리즘의 합의는 사용자와 망간의 보안 모드 협상에 의하여 실현된다.

3. 망접속 보안기능을 위한 구성 요소간의 기능 할당 모델

일부 보안기능은 아주 높은 처리능력을 요구하며, 시스템간의 신호교환은 시스템별 기능할당에 많이 좌우되기 때문에 각 시스템으로의 기능할당은 매우 중요한 사항이다. 그림 2는 IMT-2000 시스템 구성도를 보여준다. IMT-2000 이동통신시스템에서 시스템별 기능할당에서는 무선링크상의 제한된 대역폭을 고려한 신호메세지 전달의 최소화, 무선자원의 고비용 부담을 고려한 무선대역폭의 효율적인 사용, 이동단말기의 제한된 계산능력 등이 고려되어야 한다.

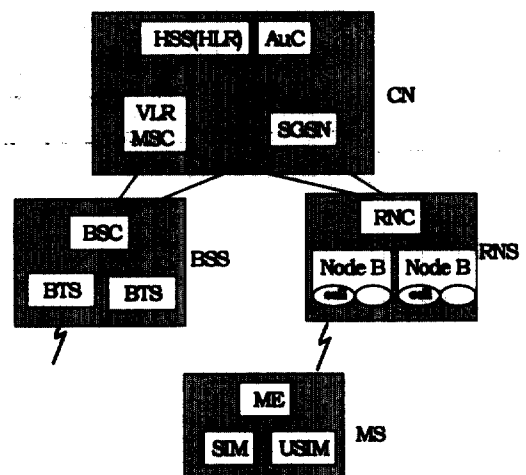
그림 3은 망접속 보안을 위한 망구성 요소간의 기능적인 흐름도를 보여준다. 이 그림에서 수직선은 망의 구성요소를 표시하며 수평선은 보안기능을 표시한다. 망접속 보안기능 중 IMT-2000에 새로이 적용되는 진전된 가입자신원 기밀성 보호 메커니즘(EUIC: Enhanced User Identity Confidentiality)은 가입자 장치인 USIM과 UIDN에서 기능이 수행되며, 기존의 가입자신원 기밀성 보호 메커니즘(UIC:User Identity Confidentiality)은 가입자장치인 UE와 VLR간, 인증 및 키 합의 메커니즘(AKA: Authentication and Key Agreement)은 HLR에 집중 시 HLR의 부하요소 및 망 내에서의 과도한 메시지흐름을 방지하기 위해 기

MS : Mobile System
BSS : Base Station System
RNS : Radio Network System
CN : Core Network

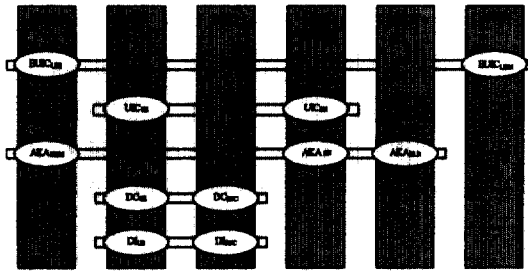
그림 2. IMT-2000 시스템 구성도

USIM : User Service Identity Module
UE : User Equipment
RNC : Radio Network Controller
VLR : Visited Location Register
HLR : Home Location Register
UIDN : User Identity Decryption Node

그림 3. 엑세스링크 보안기능 시스템 기능할당

본정보는 HLR에서 관리하고 필요 시 VLR에서 데이터를 넘겨받아 직접 가입자장치와 기능을 수행하는 것이 바람직하다. 사용자 및 신호 데이터의 기밀성 메커니즘(DC:Data Confidentiality)과 사용자 및 신호 데이터의 무결성 메커니즘(DI:Data integrity)은 AKA에서 설정된 키를 사용하여 무선구간의 종단인 UE와 RNC에서 처리하는 것이 바람직하다. 그림 4는 위의 기능할당 모델에 따른 각 구성요소별 할당된 보안기능 및 처리 알고리즘을 보여준다.

- f0 : random challenge generating function
- f1 : network authentication function
- f2 : user authentication function
- f3 : cipher key derivation function
- f4 : integrity key derivation function
- f5 : anonymity key derivation function
- f6 : user identity encryption function
- f7 : user identity decryption function.
- f8 : UMTS encryption algorithm.
- f9 : UMTS integrity algorithm.
- f10 : TEMSI calculation function
- C* : Conversion function for GSM and 3G

그림 4. 시스템별 보안기능 및 알고리즘 할당

4. 망접속 보안기능 적용에 따른 무선링크 성능 분석

본 장에서는 암호화, 인증 등 망접속 보안기능 제공에 따른 무선링크의 성능 분석을 수행한다. 보안기능의 추가에 따라 모든 구성 시스템간의 링크에서 관련 메시지 전송에 따라 부하가 증가하나 추가되는 용량의 처리가 쉽게 해결 가능한 유선구간에서의 성능분석은 제외하고 메시지 증가에 가장 민감한 구간인 무선링크에 대한 성능에 미치는 영향을 분석한다. 이를 위해 먼저 앞에서 연구된 각 시스템별 할당기능을 바탕으로 무선링크상에서 발생되는 보안 관련 메세지를 분석하고 이를 토대로 신호 및 트래픽 채널에 대한 모델을 설정하고 시뮬레이션을 통하여 보안기능이 무선채널에 미치는 영향을 분석한다.

4.1 망접속 보안 기능별 메시지용량 분석

망접속 보안 기능인 사용자 신원의 기밀성, 인증 및 키 합의절차, 데이터 무결성, 주기적인 지역 인증을 위한 신호 절차, 국부 인증 및 연결 설정 보안제어 명령 등을 위해 무선구간을 통하여 전달되어야 하는 메시지에 대하여 분석한다.

사용자 신원의 기밀성을 위해 IMT-2000에서는 각 단말에 대한 암호화 초기화 이후 임시 이동국가입자식별자(TMSI/P-TMSI)를 할당하여야 한다. 그림 3에서 본 바와 같이 이 기능은 단말의 UE와 망요소의 RNC사이에서 수행되며 할당요청 및 할당처리를 위해 무선구간 양방향에서 하나의 메시지가 필요하다. 인증 및 키 합의는 가입자에 대한 인증 수행 및 암호키 변경시 필요한 절차로서 매 호마다 필수 사항은 아니나 운용자가 지정한 시간 경과 시, 최소한 24시간 내 한번은 반드시 수행되어야 하며 무선구간을 포함하는 VLR과 UE 사이에서 신호채널을 통해 양방향 하나의 메시지가 필요하다. IMT-2000에서는 무선구간을 통과하는 모든 신호전달메시지는 전

송상의 데이터 무결성을 보장하기 위한 메커니즘이 필수적으로 요구되며 국제표준 절차에 따른 메커니즘 수행시 모든 신호메세지는 원래의 정보에 각 32비트의 정보가 추가된다.

주기적인 로컬 인증을 위한 신호절차는 망접속보안에 사용되는 COUNT값이 한계치에 도달 시 RNC에 의해 시작되며 COUNT 확인 요청 및 응답을 위해 순방향, 역방향 각 방향별 하나의 무선구간 통과 메시지가 필요하다. 국부 인증 및 연결 설정 절차는 가입자로부터 초기 계층3 메세지 수신 후(첫번째 위치등록후, 서비스요청후, 위치수정요청후, detach request 또는 연결 재설정요구후에 서비스망에 의하여 요청) 가입자와 망은 가입자인증 및 키 설정을 위한 절차가 필요하며 이를 위해 순방향, 역방향 각 방향별 하나의 무선구간 통과 메시지가 필요하다. 보안제어 명령절차는 암호절차가 필요한 경우 가입자로부터 초기 계층3 메세지 수신 후 가입자와 망간에 보안모드 요청 및 응답을 위해 각 방향 하나의 무선구간 메시지가 필요하다. 데이터 기밀성의 경우는 암호화하는 경우 plain text와 cipher text의 메시지 길이가 동일하므로 별도의 추가되는 정보나 메시지는 필요하지 않다. 표 1은 망접속보안을 위한 무선구간의 신호메세지를 보여준다.

표 1. 망접속보안을 위한 무선구간의 신호메세지

서비스 종류	메세지 용도	무선구간의 신호트래픽
기본서비스 처리메세지	· 위치등록 · 서비스요청 · 위치수정 요청 · detach request · 연결 재설정요구	· 서비스 절차에 따름
망접속보안 서비스 처리 메세지	· 사용자정보 기밀성	· 2개 메세지/서비스
	· 인증 및 키 설정	· 2개 메세지/서비스
	· 신호정보 무결성을 위한 정보	· 32bit/메세지
	· 주기적인 로컬 인증	· 2개 메세지/서비스
	· 국부 인증 및 연결 설정 절차	· 2개 메세지/서비스 (인증 및 키 합의시 외 L3엑세스시 발생)
	· 보안제어명령(서비스에 사용될 보안기능 협상)	· 2개 메세지/서비스 (L3 엑세스시 발생)
	· 데이터 기밀성	· 없음

4.2 무선신호채널 구조 및 트래픽 모델

본 절에서는 보안기능의 추가에 따른 무선링크상의 신호전송채널의 성능을 분석한다. 무선링크상의 채널은 일반적으로 신호전송과 트래픽 전송이 공유되는 inband 방식과 신호전송과 트래픽 전송이 분리되는 outband 방식으로 나눌 수 있다. 본 성능 분석에서는 비동기 방식인 3GPP의 무선접속 규격에 따라 outband 방식을 적용한다. 보안에 관련된 모든 신호메세지는 하나의 uplink 신호채널과 downlink 신호채널로 전달된다고 가정하였다. Uplink 및 downlink의 신호채널속도는 14.4, 32, 64 kbps로 가정하였다.

그림 5는 무선구간 신호채널 성능분석을 위한 채널 모델을 보여준다. 신호채널을 통하여 전달되는 신호메시지는 기본서비스를 위한 메시지와 보안기능을 위한 메시지로 분류하였다. 보안관련 메시지는 사용자신원 기밀성 처리 메시지, 인증 및 키 설정 메세지, 로컬인증 처리 메시지, 보안제어 메시지, 주기적인 로컬인증 메시지가 독립적인 메시지로 무선구간을 통해 전달되며 기본서비스를 포함한 메시지의 무결성을 수행하기 위한 추가 데이터가 모든 메시지에 필요하다. 신호정보는 메시지별로 크기는 다르나 분석의 편의성을 위하여 일반서비스 관련 메시지와 보안관련 메시지 모두 평균 메세지 크기를 256, 512, 768 bits인 경우로 가정하였다. 각 셀에 대해 발, 착신호를 포함한 기본서비스의 발생은 평균이 λ 서비스/초 인 포아손 분포를 가지며, 보안서비스는 서비스

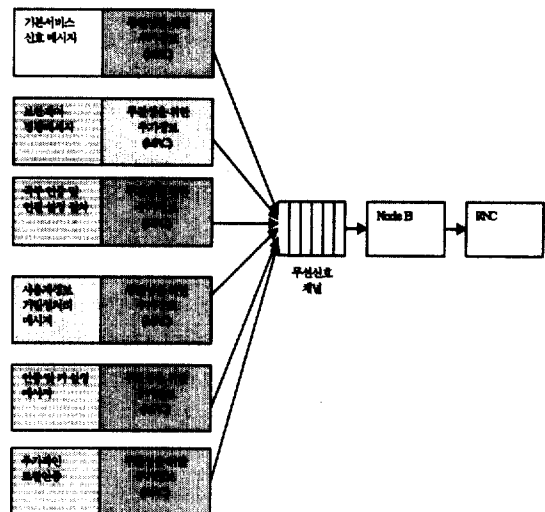



그림 5. 무선구간 신호채널 성능분석을 위한 채널 모델

특성에 따라 도달율을 달리하였으며 모두 포아손 분포로 도달한다고 가정하였다.

4.3 성능 분석 및 검토

성능분석을 위한 모델로서 각 기지국은 하나의 신호채널을 가지는 것으로 가정하였으며 기본서비스 메시지와 보안기능 관련 신호메세지는 동일한 채널을, 동일한 우선권을 가지는 것으로 가정하였다. 새로운 TMSI 할당, 인증, 암호화 키 및 무결성 키의 갱신 주기는 신호 트래픽 부하에 가장 많은 영향을 미치는 변수이나 각 운용시스템에서 운용자에 의하여 변경이 가능한 요소이다. 본 연구에서는 기지국 단위에서 발생하는 보안기능요구는 기본서비스에 비례하여 발생하는 것으로 가정하였으며 기본서비스 발생율 대비 총 보안기능 발생비율 β는 0.2에서부터 1까지 변화하는 조건에서 실험하였다.

$$\beta = \frac{\text{보안서비스 발생빈도}}{\text{기본서비스 발생빈도}}$$

성능분석은 기본서비스의 발생율이 0.2~1.0 서비스/초이고 기본서비스에 대한 보안서비스의 발생비율 β가. 0.2~1.0인 경우에 대하여 수행하였다. 기본서비스의 경우 호 당 uplink, down 링크 각 방향에 대해 신호메시지 수는 10개로 가정하였다. 여기서 기본서비스는 위치등록, 서비스요청, 위치수정 요청, detach request, 연결 재설정요구 등을 포함하며 보안서비스는 사용자신원 기밀서비스, 인증, 데이터 기밀성, 데이터 무결성 서비스와 주기적인 주기적인 로컬인증 서비스를 고려하였다.

그림 6은 메시지의 평균 메시지 길이를 256bits로 가정한 경우 망접속 보안기능 처리에 소요되는 신호메세지의 무선구간에서의 단방향 전송율을 보여준다. 기본서비스의 발생율 및 기본서비스에 대한 보안서비스의 발생비율의 증가에 따라 거의 선형적으로 증가되며 최대 1.75kbps정도의 전송율이 필요한 것으로 나타났다. 그림 7, 8은 메시지의 평균길이가 512, 768kbps인 경우를 보여주며 기본서비스의 발생율 및 기본서비스에 대한 보안서비스의 발생비율에 따른 증가는 그림 6과 동일하며 이들의 증가에 따라 거의 선형적으로 증가함을 보여준다.

그림 9, 10, 11은 각, 각 uplink 및 downlink의 신호채널 전송속도가 14.4, 32, 64kbps인 경우의 신호 메시지 차단 확률이다. 기본서비스는 0.2~1.0서비스/

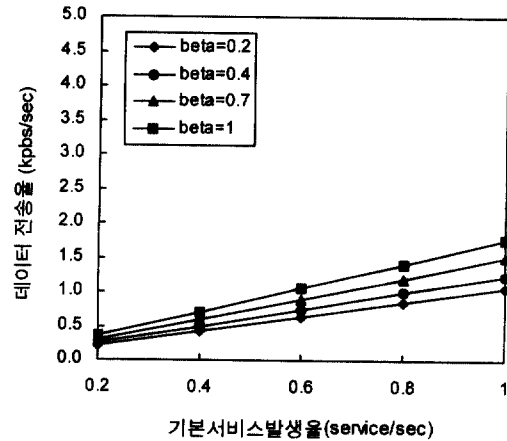



그림 6. 보안서비스를 위한 신호메세지 전송율 (평균 메시지 길이 : 256bits)

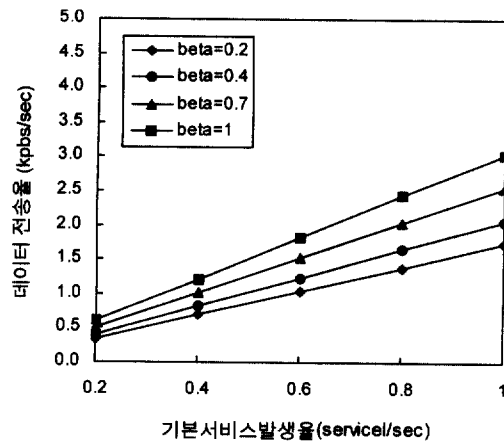



그림 7. 보안서비스를 신호메세지 전송율 (평균 메시지 길이 : 512bits)

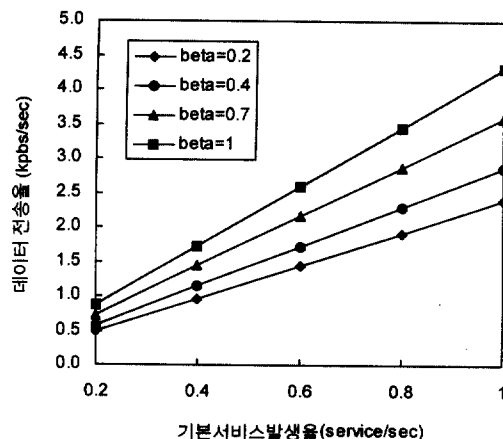



그림 8. 보안서비스를 위한 신호메세지 전송율 (평균 메시지 길이 : 768bits)

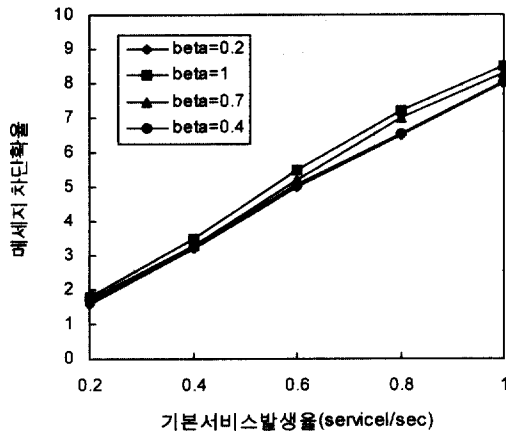



그림 9. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 14.4kbps)

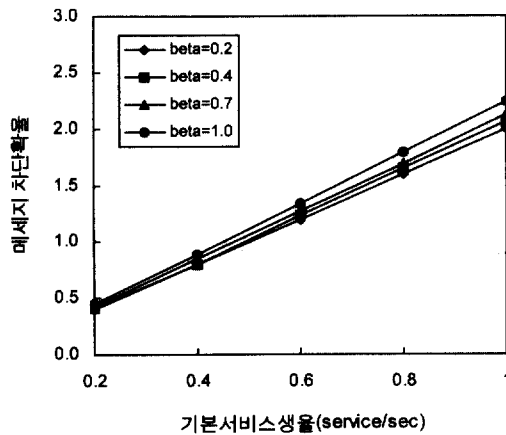



그림 10. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 32kbps)

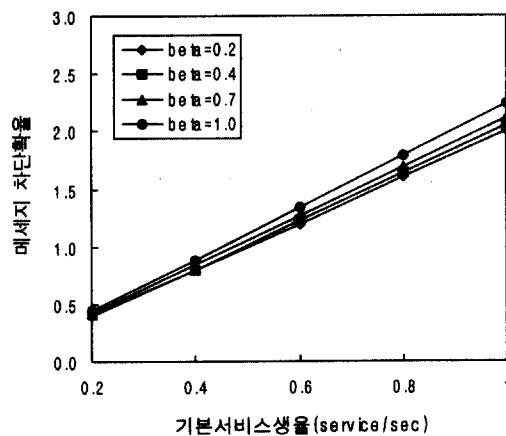



그림 11. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 64kbps)

초의 발생율로 포아손 분포를 가지고 발생하며 기본호당 신호메시지는 10개로 가정하였으며 메시지의 평균길이는 256bits로 가정하였다. 기본서비스에 대한 보안서비스의 발생비율 β는 0.2~1.0 범위에서 변화시켰다. 여기서 기본서비스는 위치등록, 서비스요청, 위치수정 요청, detach request, 연결 재설정요구 등을 포함한다. 보안서비스는 사용자신원 기밀서비스, 인증, 데이터 기밀성, 데이터 무결성 서비스와 주기적인 로컬인증 서비스를 포함한다. 그림에서 보는 바와 같이 보안 기능의 추가에 따라 무선신호채널의 블록킹 확률이 증가하며 셀의 부하와 신호채널의 용량에 상관없이 기본서비스 대비 보안서비스의 발생비율에 따라 거의 선형적으로 증가함을 볼 수 있다. 기본서비스 대비 보안서비스의 발생비율이 0.2인 조건에서 보안서비스의 제공에 따른 신호채널 블록킹 확률의 증가는 신호채널의 속도가 14.4kbps인 경우 1%, 신호채널의 속도가 32kbps인 경우 0.5%, 신호채널의 속도가 64kbps인 경우 0.25% 정도 증가하였다.

5. 결 론

현재의 2세대 이동통신시스템은 음성 서비스는 충분히 제공하고 있으나 점차 수요가 증대되고 있는 영상서비스, 무선인터넷 등 멀티미디어 서비스의 제공에는 한계를 가지고 있다. 이동멀티미디어 서비스를 제공하기 위해 3세대 이동통신시스템인 IMT-2000이 개발되고 있다.

대역폭의 확장에 따라 데이터 전송속도가 증가되는 차세대이동통신에서는 무선전자상거래 등 새로운 응용서비스가 급격히 증가될 것이다. 이들 서비스의 경우 데이터 무결성과 기밀성 보장, 부인방지(Non-repudiation), 가입자신원 익명성 등 엄격한 보안 특성을 요구한다. 그러나 IMT-2000과 같은 이동통신시스템에서는 무선링크상의 제한된 대역폭을 고려한 신호메세지 전달의 최소화, 무선자원의 고비용 부담을 고려한 무선대역폭의 효율적인 사용, 이동단말기의 제한된 계산능력 등의 제한을 가지며 이에 대한 고려가 필요하다. 본 논문에서는 IMT-2000에서 요구되는 보안기능에 대한 구조 및 기능을 분석하고 망 접속보안기능을 기능을 지원하기 위해 추가적으로 요구되는 무선구간에서의 신호트래픽의 성능

을 분석하였다. 망 접속 보안서비스의 지원에 필요한 무선구간의 신호트래픽은 평균메시지의 길이가 256~768bits, 기본서비스 대비 보안서비스 발생율이 0.2~1.0, 기본서비스의 발생율이 0.2~1.0서비스/호인 조건에서 최소 0.2kbps에서 최대 4.5kbps로 분석되었다. 신호채널의 블록킹 확률은 평균메시지의 길이가 256~768bits이고 기본서비스 대비 보안서비스의 발생비율이 0.2인 조건에서 신호채널의 속도가 14.4kbps인 경우 1%, 신호채널의 속도가 32kbps인 경우 0.5%, 신호채널의 속도가 64kbps인 경우 0.25% 정도 증가됨을 확인하였다.

본 연구의 결과는 IMT-2000시스템의 무선신호채널의 전송율 결정, 효율적인 무선 프로토콜 설계와 이동국, 기지국 등 시스템 구성 요소의 설계 및 구현에 기여할 것으로 기대된다.

참 고 문 헌

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2] s3-99005: UMTS 33.23, version 0.2.0: "Security architecture".

[3] s3-99010: Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[4] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[5] 3G TS 23.003: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".

[6] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[8] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[9] Chichun Loand Yu-Jen Chen, Secure communication mechanism for GSM networks, *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 4, 1999.

[10] AshaMehrotra etc, Mobility and Security Management in the GSM System and Some Proposed Future Improvements, *Proceeding of THE IEEE*, Vol. 86, No. 7, July 1998

[11] C. Boyd, A. Mathuria, Key establishment protocols for secure mobile communication: a critical survey, *Computer Communicatons* 23 (2000)

[12] Zao, J., etal., A Public-Key Based Secure Mobile IP, *MOBICOM97*, September 1997

권 수 근

1958년 12월 10일 생
1982년 2월 경북대학교 전자공학과 학사
1984년 2월 경북대학교 전자공학과 석사
1998년 8월 충북대학교 정보통신공학과 박사
1984년 3월~1999년 2월 한국전자통신연구원 책임연구원
1999년 3월~현재, 경주대학교 컴퓨터전자공학부 전임강사
관심분야 : 이동통신시스템, 무선인터넷, 이동망 보호 분야 등